Factors Related to Privacy Concerns and Protection Behaviors Regarding Behavioral Advertising

Factors Related to Privacy Concerns and Protection Behaviors Regarding Behavioral Advertising

Donghee Yvette Wohn
New Jersey Institute of Technology
University Heights, GITC 5500
Newark, NJ 07102 USA
wohn@njit.edu

Dan Sarkar
PACE Communications
1301 Carolina Street
Greensboro, NC 27401 USA
Dan.sarkar@paceco.com

Jacob Solomon
Michigan State University
404 Wilson Rd. Rm. 409
East Lansing, MI 48824-1212
solomon93@msu.edu

Kami E. Vaniea
Indiana University
919 E. 10th Street
Bloomington, IN 47408
kvaniea@indiana.edu

CHI'15 Extended Abstracts, Apr 18-23, 2015, Seoul, Republic of Korea
ACM 978-1-4503-3146-3/15/04.
http://dx.doi.org/10.1145/2702613.2732722

Abstract
Research on online behavioral advertising has focused on users' attitudes towards sharing and what information they are willing to share. An unexplored area in this domain is how users' knowledge of how to protect their information differs from their self-efficacy about executing privacy protection behavior. The results of a 179-participant online study show that knowledge explains privacy concerns, but self-efficacy explains protection behaviors. Perceived behavioral control was related to both concerns and behavior.

Author Keywords
Privacy; Online Behavioral Advertising; Self-efficacy; Targeted advertising; Perceived Behavioral Control

ACM Classification Keywords
K.4.1 Computers and Society: Public Policy Issues: Privacy

Introduction
Online behavioral advertising (OBA), or behavioral targeting, is "the practice of tracking an individual's online activities in order to deliver advertising tailored to the individual's interests" [2]. Advertisers like behavioral targeting because these ads have higher

click-through rates in comparison with ads that were intended for a more general audience [8]. However, targeted advertisements also raise privacy concerns with consumers who do not always like the idea of having information about what they do on the Internet recorded and retained for marketing purposes [3].

Consumers have difficulty understanding privacy policies, which are documents designed to help users understand what data will be collected about them, and how that data will be used, because they are and overly time consuming [4]. Moreover, not many people take action to protect their privacy: a 2011 TRUST-e survey found that 53% of respondents rarely or never managed their privacy choices [6].

Themes that emerged in a study of in-depth interviews with 30 adults of varying computer expertise [7] suggested that several factors were related with users' privacy protection behaviors: knowledge of how OBA works, self-efficacy, perceived usefulness of OBA, and how much control they thought they had over companies' data collection practices. This study reports results from a survey (N=179) that examined the relationships between factors that were identified from the qualitative study in regards to two aspects of privacy: users' concern about privacy, and the extent to which they tried to protect their privacy.

Privacy Protection Behaviors

Unfortunately, there is no one solution for users who want to be private online. Ad blocking plug-ins protect the user from tracking by third party advertisers, but do not protect against first party advertisers. The 'Do not track' options on major web browsers inform websites that the user does not want to be tracked, but this is only effective if the website recognizes this as a user choice. Nonetheless, despite the limitations of various types of behaviors, there is a range of different options that users can choose from to attempt to protect their privacy.

Knowledge and Self-efficacy

One factor that may affect how much people engage in privacy protection behaviors is knowledge. After all, one has to know how to do something in order to do it; in one study, only 37% said knew how to protect their personal information online [6]. Leon et al. found that users found privacy tools challenging to use and easy to set up incorrectly [3], suggesting that lack of knowledge inhibits users from engaging in privacy protection behavior:

However, on its own, knowledge may not be enough to instigate behavior if one lacks the confidence to do it. This idea of self-confidence in one's capability to do a specific behavior is defined in the academic literature as self-efficacy [1]. Bandura explains that self-efficacy drives behaviors because people have little incentive to engage in an activity if they don't think they can achieve a certain outcome [1].

In the context of privacy, researchers have found that self-efficacy explains users' attitudes about privacy. Rifon et al. [5] found that people who had high self-efficacy showed higher expectations that websites would provide information about what kind of data they were collecting if they had privacy seals, while people with low self-efficacy did not perceive differences between websites with and without privacy seals. Our main research questions, therefore, are to examine

how self-efficacy and knowledge are associated with privacy concerns and protection behaviors.

RQ. *Is self-efficacy and knowledge associated with privacy concerns and behaviors*?

Perceived Usefulness

Another perspective is that some users like receiving targeted advertisements, and therefore do not try to protect themselves despite having either knowledge or confidence enough to do so. Research studies [3] also show that some people appreciate targeted advertising if it is aligned with their interests and that people were okay with targeted advertising if they were useful [7]:

H1. *Perceived usefulness will be negatively associated with privacy concerns and behaviors*

Perceived Behavioral Control

Even if there are a wide range of options in terms of what users can do to try to prevent websites from collecting their information, or delete traces of their online activity to protect their privacy, there is also the aspect of whether or not users think their privacy behaviors will actually make a difference. For example, when a user clicks on the Ad Choices icon (www.aboutads.info/choices) they are taken to a page with multiple tabs that lists companies that are currently tracking them. Such a page may seem daunting to users and make them feel less in control of their privacy. Even users who do have a very good understanding of the technical aspects of how data are gathered and stored may perceive that what they do will not make a difference. For example, advertisers are starting to use browser fingerprints, a set of uniquely identifying facts provided by the browser to all websites visited, instead of cookies. This method is much harder to protect against, and common protections such as ad-blockers make users easier to fingerprint. Thus people who understand that their actions have a very limited impact on what information companies collect about them may be less inclined to engage in that action:

H2. *Perceived behavioral control will be positively associated with privacy concerns and behaviors*

Data collection

We recruited respondents from Amazon Mechanical Turk (MTurk). The recruiting message indicated that this was a survey about online behavioral targeted advertising. On average, respondents took a little over 9 minutes to complete the survey. Respondents were directed from MTurk to an external survey page using. After completing the survey, respondents were given a code that they could submit through MTurk to receive payment ($0.45). The attrition rate was 3.7%. The survey also included several questions designed to ensure that participants were paying adequate attention to the questions. Respondents who did not adequately answer the attention-checking questions and those who had incomplete data were removed. We were left with 179 usable responses.

Measures

Our two main dependent variables of interest were privacy concern and privacy protection behaviors. The Privacy Concern scale (M= 5.0, SD= 1.2, a= .93) was a seven-point Likert type scale by Buchanan et al.[3] that measured the extent to which the user is concerned about privacy—including online identity theft, misuse of credit card information by websites, viruses sending out emails in the user's name, etc. For the Privacy Behavior

score (*M*= 7.64, *SD*= 2.54, range from 1 to 13), participants were given a list of 14 items (see Table 1) of different privacy protection behaviors that one could engage in. The score added the number of behaviors that users said they engaged in.

Clicked on AdChoices icon	5%
Browser plugin to recommend products*	10%
Asked to opt-out of marketing data	74%
Use browser other than default	92%
Signed up to receive offers*	67%
Deleted or cleared cookies	85%
Log in to websites so they remember me*	70%
Turn off browser Javascript	23%
Turned on "Do Not Track" in browser	48%
Used Private Browsing or Incognito mode	69%

Table 1. Percentage of People Who Engaged In Particular Privacy Protection Behaviors. Items with * are reverse items.

We had four independent variables: self-efficacy, knowledge, perceived behavioral control, and perceived usefulness. Self-efficacy (*M*= 5.2, *SD*= 1.33, α= .90) was a seven-item scale asking users how confident they felt (on a seven-point Likert-type scale) in doing privacy protection-related activities. These activities included protecting privacy online, controlling who has access to their information, changing security settings of their browser, and requesting a site not to track behavior.

The Privacy Knowledge score (*M*= 4.93, *SD*= .81) was a test of 15 statements that were a mix of true and false. The score was the average of items that were answered correctly.

Perceived Behavioral Control (*M*= 4.32, *SD*= 1.33, α= .88) was a four-item scale on a seven-point Likert type scale that assessed the user's perception of how much they were able to control companies' tracking of their behavior. The items were: "I am confident that I can control what information companies collect about me," "I really don't have much control over companies tracking my information" (reverse-coded), "I feel helpless in terms of what information companies are collecting about my online activities" (reverse-coded)," and "I feel like I don't have a choice about companies tracking my online behavior" (reverse-coded).

Perceived Usefulness (*M*= 3.35, *SD*= 1.51) was three items asking users how beneficial they thought targeted advertisements were. Users rated items from "Strongly disagree" to "Strongly agree" on a seven-point Likert-type scale. The items were: "Targeted advertisements are a benefit to me," "The advantages of targeted advertisements outweigh the disadvantages," and "Overall, targeted advertisements are useful."

Results

Descriptive Statistics

Our participants were aged 18 to 62 (mean=32), and were 63% male. About 14% had a high school degree, 35.4% started college but did not graduate, 9.4% held a 2-year college degree, 34% had a college degree, and 6.7% had an advanced or professional degree. Table 1 describes the percentage of respondents who engaged in behaviors that were towards or counter to protecting their information from companies.

	Beta	t
Age	-.09	1.24
Gender	.10	1.39
Education	.18*	2.56
Perceived Usefulness	-.11	-1.51
Perceived Behavioral Control	.29**	.35
Self-efficacy	.14	1.65
Knowledge	.30***	3.98

*Coefficients are standardized, *p<.05, **p<.01, ***p<.001*

Table 2. OLS Regression Explaining Privacy Concerns

	Beta	t
Age	.05	.66
Gender	.04	.57
Education	-.07	-1.03
Perceived Usefulness	-.04	-.58
Perceived Behavioral Control	.22**	2.69
Self-efficacy	.49***	5.73
Knowledge	.06	.83

*Coefficients are standardized, *p<.05, **p<.01, ***p<.001*

Table 3. OLS Regression Explaining Privacy Protection Behaviors

Hypothesis Testing

To test our hypotheses for privacy concern, we ran an Ordinary Least Squares (OLS) regression, with perceived usefulness, perceived behavioral control, self-efficacy, and knowledge as independent variables and privacy concern as our dependent variable (Table 2). After controlling for gender, age, and education, our model was statistically significant, $F(7, 172)= 5.22$, $p<.001$, adjusted $R^2= .14$. Among the demographic variables, only education was statistically significant; users who were more educated were more likely to have higher concerns about their privacy. Perceived behavioral control was also a positive predictor; users who felt they had higher control of their own behaviors were more likely to have higher privacy concerns. Self-efficacy did not statistically show any relationship with privacy perception. However, higher knowledge of the technical aspect of behavioral advertising was correlated with higher privacy concern.

The regression model predicting privacy behavior was significant, $F(7, 172)= 6.52$, $p<.001$, adjusted $R^2 =.18$. Self-efficacy was a strong, positive predictor of behavior; those who had higher confidence were more likely to engage in privacy behaviors. Perceived behavioral control was also positively correlated with their privacy behaviors—people who thought that their privacy behaviors would make a difference engaged in those behaviors. Knowledge, however was not significantly related to privacy behaviors (Table 3). Perceived usefulness was not statistically related with either privacy concerns or behavior.

Conclusion

Online behavioral advertising is a practice in which users' online activities are collected and utilized to deliver them customized advertisements. We found that actual knowledge of how OBA works was significantly related to how concerned they are about their privacy. However, more knowledge was not correlated with engaging in more privacy protection behavior. It was self-efficacy—users' level of confidence about being able to protect themselves—that contributed to the extent to which the user actually engaged in preemptive or reactive behaviors to protect their privacy.

It is important to note that engaging in behaviors to protect one's privacy is not akin to actual protection. However, the fact that the knowledgeable users were not actually engaging in privacy protection behaviors suggests that they think that their actions will have little effect on companies. Users who had higher perceptions of control over what information companies were collecting were the ones more likely to engage in privacy protection behaviors.

Policy Implications

This finding is particular important to take into consideration for future policies. Most of the effort to date has focused on making information accessible to users and requiring websites to make more clear what kind of information they are collecting. Those efforts should continue, but in addition, more focus could be to have companies provide more guidelines to users about what users can to do prevent corporate data collection. Efforts may also be made to ensure that users can be more selective about the information that companies store. This may alleviate knowledgeable users' feeling of helplessness, but at the same time easy instructions and education may need to be provided to increase

self-efficacy of those who do not have much knowledge regarding the technical aspects of OBA.

Design Implications

From a design perspective, our results suggest that if we want users to engage in more privacy protection behavior, systems need to make clearer to the users that they can prevent targeted advertising. Our users reported never clicking on the "I" icon, which is consistent with Leon et al. [3] which found that users were not effectively using privacy tools. If this is the primary method that advertisers have for users to protect themselves, it should be made more salient. The privacy protection products are not serving users well [3]; this study furthers existing findings in that we see that knowing the technical aspects of how targeted advertising works is not enough to engage in privacy protection behaviors. This means that either the solutions need to provide feedback to end users that they are effective (improve perceived control for knowledgeable users), or make using them sound more possible (improve self-efficacy).

Future Work

These results also raise several important questions for future research. Since self-efficacy and perceived behavioral control predict privacy behaviors, it is important to learn how people develop self-efficacy and perceived control over their privacy from OBA. Also, why was self-efficacy not related to privacy concerns? Is this because those with high self-efficacy feel they have taken the necessary steps to be protected? If so, this self-efficacy may be creating a false sense of security. Answering these questions will be important for developing designs and policies that better help users protect their privacy when using OBA.

References

[1] Bandura, A. Self-efficacy: toward a unifying theory of behavioral change. *Psychological Review 84*, 2 (1977), 191–215.

[2] Federal Trade Commission. Self-regulatory principles for online behavioral advertising. 2009.

[3] Leon, P., Ur, B., Shay, R., Wang, Y., Balebako, R., and Cranor, L. Why Johnny can't opt out: A usability evaluation of tools to limit online behavioral advertising. In *Proc. CHI 2012*, ACM Press (2012), 589–598.

[4] Mcdonald, A.M. and Cranor, L.F. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society* (2008).

[5] Rifon, N.J., LaRose, R., and Choi, S.M. Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. *Journal of Consumer Affairs 39*, 2 (2005), 339–362.

[6] TRUSTe. Online behavioral advertising (OBA) privacy. 2011.

[7] Wohn, D. Y., & Sarkar, C. The uncanny valley effect in behavioral targeting and information processing of peripheral cues. In *Proc. iConference* (2014), 577-582.

[8] Yan, J., Liu, N., Wang, G., Zhang, W., Jiang, Y., and Chen, Z. How much can Behavioral Targeting Help Online Advertising? *Distribution 7*, 2 (2009), 261–270.